BY ORDER OF THE SECRETARY
OF THE AIR FORCE

AIR FORCE INSRUCTION 10-1703
VOLUME 3

6 MAY 2015

Operations

CYBERSPACE OPERATIONS
AND PROCEDURES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available for downloading or ordering on the e-Publishing website at **www.e-publishing.af.mil**

RELEASABILITY: There are no releasability restrictions on this publication

OPR: AF/A3CO/A6CO

Certified by: AF/A3C/A6C
(SES Peter E. Kim)
Pages: 11

This instruction implements Air Force (AF) Policy Directive (AFPD) 10-17, Cyberspace Operations, and establishes AF-wide basic procedures for the operation of cyberspace weapons systems approved by the Chief of Staff of the AF. This publication applies to all military and civilian AF personnel, members of the AF Reserve Command (AFRC), Air National Guard (ANG), and contractor support personnel in accordance with appropriate provisions contained in memoranda support agreements and AF contracts. The authorities to waive wing/unit level requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. See AFI 33-360, Publications and Forms Management, Table 1.1 for a description of the authorities associated with the Tier numbers. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, Recommendation for Change of Publication; route AF Form 847s from the field through Major Command (MAJCOM) publications/forms managers to AF/A3C/A6C and AF/A6S. Ensure all records created as a result of processes prescribed in this publication are maintained in accordance with AF Manual (AFMAN) 33-363, Management of Records and disposed of in accordance with the AF Records Disposition Schedule (RDS) located in the AF Records Management Information System (AFRIMS).

1. General.

1.1. Overview. This instruction establishes procedures for personnel assigned to AF cyber weapon systems.

1.2. Specific Applicability. This instruction applies to all personnel who operate AF cyber weapon systems and/or their related equipment. Personnel performing cyberspace operational support or maintenance functions will comply with appropriate guidance in Methods and Procedures Technical Order (MPTO) 00-33A-1001, General Communications Activities Management Procedures and Practice Requirements, AFI 33-150, Management of Communications Activities, and/or AFI 36-2201, Air Force Training Program, as applicable. Cyberspace Combat Mission Ready (CMR) certification applies to all military and civilian personnel who have completed Undergraduate Cyber Training/Cyber Defense Operations Course, 39 IOS Initial Qualification Training (IQT) (if available) and Mission Qualification Training (MQT), have passed an evaluation and are certified by an appropriate certifying official. CMR requirements may apply to additional personnel at selected units at the direction of AF Space Command (AFSPC)/A3. (T-2)

1.3. Supplements. Major Commands (MAJCOMs)/Numbered Air Forces (NAF)/Wings/Groups/Squadrons may supplement this instruction to provide specific guidance to their aligned units in accordance with AFI 33-360. The Headquarters AF Directorates of Cyberspace Operations and Warfighting Integration (A3C/A6C) and Cyberspace Strategy and Policy (AF/A6S) will review and coordinate on all supplements to this instruction. Air Reserve Components (ARC) will provide a copy of any approved supplement to AF/A3C/A6C, AF/A6S, and AFSPC/A3.

1.4. Real-Time Operations & Innovation (RTOI). RTOI projects are operational rather than acquisition-related activities. The RTOI construct enables the USAF to generate tools and tactics in response to critical cyber needs at the fastest possible pace.

1.4.1. RTOI activities are specifically intended to satisfy urgent and short-term operational needs in response to:

1.4.1.1. Cyber Incidents/Events Category 0 thru 9, as outlined in the Chairman of the Joint Chief of Staff (CJCS) Instruction 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), and CJCS Manual 6510.01B, Cyber Incident Handling Program. Emergent threats and opportunities as determined by 24 AF/CC.

1.4.1.2. Newly discovered critical vulnerabilities not currently mitigated within the Air Force Enterprise network or capable of remediation by other means.

1.4.1.3. Critical cyberspace operational needs (both defensive and offensive), which 24 AF/CC has been tasked to fulfill or which have been identified through the conduct of daily operations.

1.4.2. RTOI complements the traditional acquisition framework, providing responsive technical solutions to urgent cyber needs which cannot be fulfilled by Rapid Acquisition (RA) or Foundational Acquisition methods. It is not intended to circumvent normalized operational and acquisition processes through informal relationships among the United States Cyber Command, the Armed Forces, the National Security Agency, and the Defense Information Services Agency. HQ AFSPC will develop specific policy for quick-reaction processes otherwise available for the rapid fielding of capabilities. (T-2)

1.5. Crew Responsibility. In conjunction with other governing directives, this instruction prescribes operations procedures for cyberspace weapons systems under most circumstances, but it is not a substitute for sound judgment or common sense, . As a general rule, except as noted in paragraph 3.5.1. or in guidance that states an action “must” or “shall” be carried out, operations or procedures not specifically addressed in this instruction may be accomplished if they enhance safe, effective mission accomplishment and are approved for execution by appropriate command authorities.

1.6. Waivers. Unless otherwise specified, AFSPC/A3I is the waiver authority for this instruction; this authority may be delegated to the wing commander level within AFSPC, but no lower.

1.6.1. Waiver requests which must be approved by HQ AFSPC/A3I will be appropriately classified and submitted in memo or message format to the 24 AF Operations Directorate (24 AF/A3/5) via channels appropriate to the level of classification; classified requests should be submitted to **24af.a3@lackland.af.smil.mil**, with copies to HQ AFSPC/A3I (**afspc.a3i.wf@afspc.af.smil.mil**) and HQ USAF/A3C/A6C (**usaf.pentagon.saf-cio-a6.mbx.a6c-a3c-workflow@mail.mil**). 24AF/A3/5 will recommend approval or disapproval; approved waiver requests will be forwarded to AFSPC/A3I for final approval. Each waiver request will include, at a minimum, the following information:

1.6.1.1. The specific requirement to which the waiver request responds.

1.6.1.2. Full justification/rationale for the waiver request.

1.6.1.3. The proposed waiver expiration date/time.

1.6.2. Approved waivers are valid for a maximum of one year from the effective date.

1.6.3. ARC units will forward waiver requests which cannot be granted at the wing commander level through command channels to the applicable MAJCOM Operations Division (e.g., ANG/A3C or AFRC/A3), for approval. Approved waivers are valid for a maximum of one year from the effective date. Provide information copies of approved waivers to AF/A3C/A6C, AFSPC/A3, and the ARC MAJCOM OPRs.

1.7. Changes and Clarifications. The HQ AF Director of Cyberspace Strategy and Policy (AF/A6S) has overall authority for administration of this instruction.

1.7.1. Recommend changes to this publication using AF Form 847. Coordinate and route AF Forms 847 through the unit's chain of command to AFSPC/A3I, **afspc.a3i.workflow@us.af.mil**, which will forward approved change proposals to AF/A6SS, 1480 Air Force Pentagon, Washington, DC, 20330-1480 (or via electronic message to AF/A6S Workflow, **usaf.pentagon.saf-cio-a6.mbx.a6s-workflow@mail.mil**), for final review and approval.

1.7.2. Process requests for clarification via memorandum or message to AFSPC/A3I through 24 AF/A3/5, **24af.a3@us.af.mil.** 24 AF will provide the NAF position prior to forwarding.

1.7.2.1. If a clarification request was initiated by telephone, the submitting unit will follow up in writing within one working day. (T-3)

1.7.2.2. AFSPC/A3I will route the response back to the requestor through 24 AF/A3/5.

2. Mission Planning.

2.1. Responsibility. Individual crews, unit operations, and intelligence functions jointly share responsibility for mission planning. The crew commander/senior crew member is ultimately responsible for all aspects of mission planning to include complying with command guidance. Unit commanders may establish weapon system specific mission planning requirements but will ensure an appropriate level of mission planning is conducted prior to each mission. (T-1)

2.2. Procedures. Effective mission accomplishment requires thorough mission planning and preparation. Failures in execution often result from poor mission preparation, therefore units will conduct thorough planning prior to every mission. General mission planning considerations are addressed in AFTTP 3-1, General Planning, and CWO specific planning consideration can be found in AFTTP 3-1, Cyber Warfare Operations, or other weapon system specific AFTTP 3-1 volumes. While not directive, these manuals are useful in ensuring adequate mission planning and employment. (T-1)

2.2.1. Units will accomplish sufficient planning to ensure successful mission accomplishment for all phases of operations. The mission commander/senior crew member will use the Plan-Brief-Execute-Debrief (PBED) process for mission planning. At a minimum, mission planning will include mission objectives, expected threats (identity and counter-tactics), weapons delivery, cancel/abort/rollback criteria and/or contingency plans, Rules of Engagement (ROE), Risk Management (RM), lessons learned and applicable Special Instructions (SPINS). (T-2)

2.2.2. Unit staff will provide crews sufficient time and resources to accomplish crew mission planning and mission briefing. Mission planning must be accomplished by members who understand the capabilities and limitations of their weapon system, in a realistic training and/or mission rehearsal environment. Unit staff will ensure other activities, such as recurring academic training, training device periods, additional duties, etc., do not interfere with time allotted for mission planning and crew mission briefing. The crew commander/senior crew member is ultimately responsible for the proper conduct of mission planning and must ensure sufficient time and materials are available to effectively plan the mission. (T-2)

2.2.3. Crew substitutions require approval by unit operations officer or higher. Crew substitutions may be made as long as the substitute crewmember is thoroughly briefed and understands all aspects of the mission. (T-3)

2.3. Crew Mission Planning. Detailed crew mission planning helps ensure mission objectives are understood by all crew members and an effective plan is developed to achieve those objectives. In preparation for and prior to each sortie, crews will take tactical objectives provided by higher headquarters organizations through tasking orders and create tactical tasks for execution in the next sortie.

2.3.1. All crew members must be present during shift change or sortie briefing unless specifically excused by the squadron operations officer or higher authority. The crew commander/senior crew member will direct detailed mission planning, including procedures to employ. Crew commander/senior crew member will review all crew and crewmember training requirements and currency data to the maximum extent possible;

review crew and weapon system restrictions for each activity planned and plan an alternate mission/activity in the event equipment failure prevents accomplishing the primary mission. (T-3)

2.3.2. The crew commander/senior crew member is ultimately responsible for ensuring the adequacy and completeness of all mission data and resources and must make risk determinations to cancel or abort missions. The crew commander/senior crew member must ensure crew substitutions are made in time for the substitute crewmember(s) to be thoroughly briefed and familiar with the applicable mission data available and to rehearse with the rest of the crew in realistic range/training facilities, as required**.** (T-2)

2.4. Weapons and Tactics. Weapons and Tactics personnel will support the employment of current/effective TTPs, the planning/briefing/execution/debriefing of missions, and development of lessons learned. (T-2)

2.5. Intelligence and Threat Study. During mission planning, crews will receive a current intelligence briefing which will include detailed briefings on current adversary activity, threat type and capabilities. Crews will also review applicable TTPs and implement in accordance with mission requirements. (T-2)

3. Normal Operations.

3.1. Crew Logs. The crew log is the official record of events that occur during a crew shift or sortie (live or simulated). The purpose of the log is to maintain an accurate and detailed record of all significant events, including any deviations from guidance in this Instruction pertaining to operations occurring during each crew shift. Of primary importance are events that may result in subsequent investigations. At a minimum, crew logs will include identification of on-duty personnel, major operational activities, significant communications, major system degradations and other abnormal system responses**.** Maintain crew logs for one year to provide historical reference for mission operations. (T-3)

3.2. Crew Information File (CIF). The CIF provides information essential to the conduct of normal operations and response to emergency conditions. The CIF centralizes significant, time-sensitive issues and ensures procedures are disseminated to operations personnel. All crew members are required to review the CIF and acknowledge completion prior to beginning crew duties. Refer to AFI 10-1703, Volume 1, Cybercrew Training, for information on the structure and content of the CIF**.** (T-3)

3.3. Crew Shift/Mission Briefing. A successful mission briefing covers objectives tasked by higher headquarters, assigns tactical tasks to achieve those objectives, and ensures all crew members understand the plan.

3.3.1. The crew commander/senior crew member will conduct a crew mission briefing and rehearsals as necessary for all missions. When rehearsals confirm mission feasibility, the responsible commander approves the mission plan and authorizes execution. Crews will practice, mission plan and modify operational details according to rehearsal results. (T-3)

3.3.2. A crew member excused from the mission briefing, or substituted following the briefing, must receive a detailed briefing from the crew commander/senior crew member and be afforded an opportunity to rehearse his/her role with other crewmembers, as required. (T-3)

3.4. Shift/Mission Debriefing. The crew commander/senior crew member will lead a thorough mission debrief for every mission. The mission debrief will cover the following at a minimum: whether tasks and objectives were met, lessons learned, and learning points. (T-3)

3.5. Checklists, Local Procedures, and Crew Aids.

3.5.1. Crew members will strictly adhere to all checklists in a technical order (TO), all unit generated checklists or other higher headquarters (HHQ) directives. (T-2)

3.5.2. 24 AF/A3 will generate guidance to cover actions not addressed in a TO or other directives. (T-2)

3.5.3. Units may develop local procedures specific to their mission when operations fall outside existing TOs and HHQ guidance. Local procedures will not be used to re-create or consolidate existing technical data or HHQ guidance. (T-3)

3.5.4. Crew members may develop local crew aids such as charts, question banks, guides or other visual aids and processes to bolster proficiency, enhance changeover briefings and to ensure comprehensive tasks are completed correctly. However, these aids will not override or be used in lieu of TOs and other directives. The squadron commander will review and recommend approval/disapproval of all locally developed crew aids. Local crew aids will be approved by the Group commander or his/her designee. (T-3)

3.5.5. Briefing Guides. Units will develop local briefing guides to ensure all necessary items are covered prior to each mission. Group-level Stan/Eval, or designated stan/eval entity, will determine minimum requirements for these guides and ensure standardization. (T-3)

3.5.5.1. Guides will contain procedural guidance addressing mission accomplishment with abnormal/degraded/inoperative equipment. (T-3)

3.5.5.2. Guides will contain other information deemed necessary by individual units, i.e., local training procedures, and procedures for notifying maintenance personnel of equipment discrepancies. (T-3)

4. Operational Tests and Exercises. Exercising, testing and evaluating the crew force is necessary to maintain proficiency; however, exercises and tests also provide important data needed to validate the operation of the weapon system. (T-3)

4.1. During an exercise or test, crewmembers will and follow established operating procedures, AFIs, and governing publications with the understanding that exercise and tests are an avenue to try new TTPs and capabilities. RM should be performed at all levels to mitigate any risk. (T-3)

4.2. Exercises and tests will not jeopardize real-world missions. Real-world emergencies or priorities may require a crew to withdraw from a test or exercise. The crew commander/senior crew member will coordinate with the unit commander or operations officer and all other participating agencies to cancel, postpone or withdraw from a test or exercise. (T-3) When priority actions are complete, the crew may be permitted to resume participation as approved by appropriate authorities.

5. Crew Force Management.

5.1. Crew Rest, Fatigue Management and Duty Limitations. This section prescribes mandatory crew rest and maximum duty periods (DP) for all personnel who operate AF cyberspace weapon systems. Basic guidance for fatigue management strategies and waiver authority procedures are also addressed**.** (T-3)

5.1.1. The normal crew DP should not exceed 12 hours. (T-3)

5.1.2. When authorized by the appropriate group commander, the crew commander/senior crew member may extend the maximum DP up to two hours to compensate for unplanned mission delays, provided the mission requirements justify the increased risk. Extended DP must be annotated in the mission log, at a minimum detailing authorizing official (i.e., group commander or designated representative) and crew members affected. Mission or environmental needs requiring longer than a 14 hour DP require wing commander approval (may be delegated to OG/CC or equivalent). (T-3)

5.1.3. Regardless of authorized DP, the crew commander/senior crew member will restrict duty time, extend crew rest periods, notify squadron leadership to generate alternate crews, or terminate a mission if safety may be compromised by fatigue factors. (T-3)

5.1.4. DP begins when a crew member reports for a mission/sortie, briefing, or other official duty and ends with the completion of the mission debrief. (T-3)

5.1.5. The crew rest period is a 10-hour non-duty period before the DP begins. Its purpose is to ensure the crew member is adequately rested before performing a cyberspace mission or mission-related duties. Crew rest is free time, and includes time for meals, transportation and the opportunity for eight hours of uninterrupted sleep. (T-3)

5.1.6. Crew rest is compulsory for any crew member prior to performing any crew duty on any cyber weapon system. (T-3)

5.1.7. Each crew member is individually responsible to ensure he or she obtains sufficient rest during crew rest periods. (T-3)

5.1.8. Any official business or duty that requires the active participation of a crew member, not during the DP, interrupts the crew rest period. This includes official business conducted via telephone or other electronic means. If crew rest is interrupted so that the individual cannot get an opportunity for at least eight hours of uninterrupted sleep, the individual must be afforded the opportunity for at least eight more hours of uninterrupted sleep plus reasonable time to dress, eat, travel, etc. Intentional crew rest interruptions shall only be made under the most exceptional circumstances. The individual must consider unofficial interruptions so that the intent of this section is met. If crew rest is interrupted, individuals will inform a supervisor and remove themselves from the mission schedule, when necessary. (T-3)

5.1.9. Exceptions to the 10-Hour Minimum Crew Rest Period. For continuous operations when basic crew DPs are greater than 12 but less than 14 hours, subsequent crew rest may be reduced proportionally to a minimum of 10 hours to maintain a 24-hour work/rest schedule. (T-3)

5.1.10. Continuous operations is defined as two or more consecutive DPs of at least 12 hours duration separated by minimum crew rest. (T-3)

5.1.11. The 10-hour crew rest exception shall only be used to keep crews in 24hour clock cycles, not for scheduling convenience and will not be sustained for more than 72 hours. (T-3)

5.1.12. Any reduction from 10 hours crew rest requires pre-coordination for transportation, meals and quarters as necessary so crewmembers are provided an opportunity for at least eight hours of uninterrupted sleep. (T-3)

5.1.13. Crew members will not perform cyberspace mission duties within 12 hours of consuming alcohol or other intoxicating substances, or while impaired by its after effects. (T-3)

5.2. Crew Scheduling. Crew scheduling will be accomplished in accordance with crew rest limitations provided in this guidance. (T-3)

5.2.1. Maintain crew integrity to the maximum extent possible.

5.2.2. Units should attempt to provide all crewmembers a stable schedule using a standard rotation for 24/7 crews to the maximum extent possible.

5.2.3. Operations Scheduling. Operations schedulers will publish, post and monitor schedules for the crew force and initiate changes to the schedules based on tracking of qualifications, certifications, restrictions and other factors as required to meet mission objectives. (T-3)

5.2.3.1. Operations schedulers will make schedule change notifications within 24 hours for changes that take effect within the next 72 hours. Make notifications as soon as practical after the change is official, but not later than 12 hours prior to the scheduled event time. (T-3)

6. Operations Review Board (ORB). MAJCOMs/NAFs will establish an ORB process for conducting investigations to determine the cause of any mission failures or significant events, including abnormal system responses or trends. If the initial analysis reveals the incident is outside the purview of the affected Wing, then the parent MAJCOM may request ORB support from HQ AFSPC. In cases where the responsible organization does not have the required expertise, the MAJCOM can request that expertise through HQ AFSPC. Exceptions can be worked on a case by case basis through MAJCOM to MAJCOM interaction, with appropriate support from all interested parties. Examples of circumstances requiring an ORB include: Major system degradation, indications of erroneous system response/procedures with significant mission impact and significant events where the cause cannot be determined by initial assessment or when corrective action is beyond minimal retraining or minor procedural changes. A significant, abnormal system response may include major hardware or software anomalies, safety violations, or security deficiencies.

TOD D. WOLTERS, Lt Gen, USAF
DCS, Operations, Plans & Requirements

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

National Military Strategy for Cyberspace Operations, December, 2006

DoDD O-3600.01, Information Operations, 2 May 2013

DoDD O-8530.1, Computer Network Defense (CND), 8 January 2001

DoDI O-8530.2, Support to Computer Network Defense (CND), 9 March 2001

Joint Publication 3-12, Cyberspace Operations, 5 February 2013

CJCSI 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND), 9 February 2011

CJCSM 6510.01B, Cyber Incident Handling Program, 10 July 2012

AF Doctrine Annex 3-12, Cyberspace Operations, 15 July 2010, with Change 1, 30 November 2011

AFPD 10-17, Cyberspace Operations, 31 July 2012

AFI 10-710, Information Operations Condition (INFOCON), 10 August 2006

AFI 10-1701, Command and Control for Cyberspace Operations, 5 March 2014

AFI 10-1703V1, Cybercrew Training, 2 April 2014

AFI 33-360**,** Publications and Forms Management, 25 September 2013**.**

AFI 91202, The US Air Force Mishap Prevention Program, 5 August 2011

AFMAN 33-363, Management of Records, 1 March 2008

AFTTP 3-1, Tactical Employment Cyber Warfare Operations, 26 Apr 12

AFTTP 3-1, General Planning, 6 Feb 14

Methods and Procedures Technical Order (MPTO) 00-33A-1001, *General Communications Activities Management Procedures and Practice Requirements*.

TASKORD 14-005, Operation COBALT NEEDLE (OCN), 8 Apr 14

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

AF—Air Force

AFI—Air Force Instruction

AFPD—Air Force Policy Directive

AFRC—Air Force Reserve Command

AFSPC—Air Force Space Command

AFTTP—Air Force Tactics, Techniques, and Procedures

ANG—Air National Guard

ARC—Air Reserve Component

C2—Command and Control

CIF—Crew Information File

CJCSI—Chairman, Joint Chiefs of Staff Instruction

CJCSM—Chairman, Joint Chiefs of Staff Manual

CMR—Combat Mission Ready

CND—Computer Network Defense

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DP—Duty Period

HQ—Headquarters

IMSC—Installation and Mission Support Center

IQT—Initial Qualification Training

ISR—Intelligence, Surveillance, and Reconnaissance

JP—Joint Publication

MAJCOM—Major Command

MPTO—Methods and Procedures Technical Order

MQT—Mission Qualification Training

OC—Operations Center

OPR—Office of Primary Responsibility

RM—Risk Management

RTOI—Real-Time Operations and Innovation

SA—Situational Awareness

SPINs—Special Instructions

TO—Technical Order

USAF—United States Air Force

Terms

Cyberspace Operations.—The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. (JP 3-12)

Information Assurance (IA).— Measures that protect information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation.

Network Operations (NetOps).— Activities conducted to operate and defend the Global Information Grid. (JP 6-0)

Sortie.— A cyber sortie (combat or training) constitutes the actions an individual cyberspace force package takes to accomplish a tasked mission. The base unit for a sortie is a cyberspace force package. A cyberspace force package completes a single sortie when it comes “off station” or the tactical commander declares a “knock it off”. Missions may require multiple cyberspace force packages to conduct multiple sorties in order to accomplish mission objectives. (TASKORD 14-005)